

June  
2011

MONTHLY  
Cyber Security  
Newsletter

# Security Tips

## What's new this month?

This month we will look deeper into the mystery of cyber forensics as well as look at several pointers to help in protecting your home network.

Mississippi Department  
of Information  
Technology Services

Division of Information Security

## What Is Computer Forensics

Greg Nohra and Jay White

When I think of computer forensics, an image of David Caruso slowly taking off his sunglasses quickly pops into my mind. David Caruso plays the role of Horatio Caine, the leader of a team of forensic investigators/police officers who use both cutting-edge scientific methods and old-fashioned police work to solve crimes on the TV series CSI: Miami. In reality, the link between computer forensics and the general plot of the CSI: Miami TV series is not that implausible. In fact, there are many separate forensic disciplines ranging from forensic arts to forensic polymer engineering. Forensics is defined as a science that deals with the relation and application of a particular field. Computer forensics is a branch of digital forensic science pertaining to the legal evidence found in computers and digital storage media. As computer technology becomes more prevalent in our society, the need for computer forensic knowledge and experience will be viewed more as a requirement than a luxury.

So, what is computer forensics? The goal of computer forensics is to examine computer evidence stored on a computer in a forensically sound manner with the aim of preserving, collecting, validating, identifying, analyzing, interpreting, documenting and presenting facts and opinions about the evidence/information. Computer forensics is instrumental during a computer incident, whether it is the identification of an intruder on an organization's network or gaining insight into events such as theft of intellectual property or criminal matters. The highest profile incidents usually involve criminal investigation or civil litigation, but computer forensic techniques can be of value in a wide variety of situations, including attempts to retrieve data that has been inadvertently deleted, recover a forgotten password, or document a list of websites that have been visited. If anyone has spent any substantial amount of time on a computer or has the responsibility of maintaining a family computer, it is very likely that they have used some rudimentary computer forensic skills to investigate problems

The science of computer forensics seems to be fairly straightforward; however, a computer forensics examination for an organization can be a complicated process that requires a number of skills and tools to obtain credible and reliable evidence that will clearly and factually answer the questions of “who, what, when, where and how” as it relates to a specific incident.

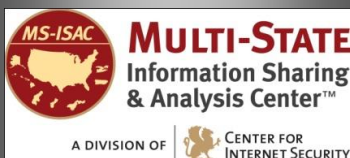
An organization’s ability to practice sound computer forensic technique will help ensure the overall integrity and survivability of their network infrastructure. Understanding the legal and technical aspects of computer forensics will help the organization capture vital information if their network is compromised and will help them legally if the intruder is caught. If an organization ignores the fundamentals of computer forensics they run the risk of destroying important evidence or having the forensic evidence ruled inadmissible in a court of law. Also, if an organization remains uneducated about the proper techniques of computer forensics, the organization could potentially be held liable in civil or criminal court for failing to protect certain types of data.

When an organization is preparing to conduct a computer forensics investigation, the organization must consider any already-known facts about the incident to determine the appropriate strategy. An incident involving the defacement of a website will need to be handled differently than one involving recovery of web-browser history, because the type of evidence expected to be collected will be different. This potential evidence will fall into one of two basic categories of data that can be collected, persistent and volatile. Persistent data is data that is stored on a local hard drive or other medium that is preserved when the computer is powered off. Volatile data is any data that is stored in memory, or exists in transit, that is lost when the computer is powered off. These two types of data require different types of tools to investigate incidents. An organization’s ability to quickly and effectively obtain detailed information regarding an incident will have a direct impact on the success or failure of a computer forensic investigation.

Every organization should be aware of the most stringent aspect of any forensic investigation, the legal implications. Because the investigation may result in legal ramifications, the organization should work methodically and always strive to preserve the original evidence. In most cases it is suggested that any investigative work be performed on a duplicate of the original data, to prevent the original from being altered or destroyed. Working from a duplicate will also help the organization demonstrate that they have maintained the integrity of the evidence throughout the process. Maintaining (and proving) the integrity of the evidence from the initial point of collection is paramount to any computer forensics investigation.

As mentioned earlier, a computer forensic investigation can be a very complicated process. An organization’s ability to gather and analyze evidence in a forensically sound manner and to comprehend the legal concepts of computer forensics will prove to be a benefit to the organization. Organizations that are not prepared to follow the proper protocols of a computer forensic investigation have a significant amount to lose. When CSI: Miami’s David Caruso is faced with a new investigation, he slowly and calmly removes his sunglasses with the confidence that he will be able to solve the crime. When facing a potential computer forensic investigation, does your organization have this same confidence?

this newsletter is  
brought to you  
by...



[www.msisac.org](http://www.msisac.org)



[www.its.ms.gov/  
services\\_security.shtml](http://www.its.ms.gov/services_security.shtml)

## Protecting Home Networks/Computers

AliceClaire Thompson

According to F-Secure, an antivirus software company, 80% of home computers are infected with spyware or adware programs and about 67% of home computers lack current antivirus software. With the rapid growth of new intrusion tactics and viruses, home users need to be more educated than ever before on security measures to take in order to protect their home computers and networks. Listed below are some actions that can be taken in order to make your home network environment more secure and protected against cybercriminals:

1. **Install a firewall** – A firewall is a software program or a hardware device that limits connections to your computer or network. Your firewall should be configured in the most-specific way possible, so that unnecessary ports are not accessible from the Internet. Some operating systems have software firewalls installed, but many of them may default to the “off” mode, so make sure that your firewall is turned on. No firewall will block all attacks so it is not enough to install a firewall and then ignore all other security measures.
2. **Secure your wireless connection** – Change your SSID from the default and don’t broadcast it. Change the default password of the admin interface of your wireless router. Enable, at minimum, WPA encryption with a strong password. The encryption will both restrict access to your network and protect your data during transmission.
3. **Install and maintain anti-virus software** – Anti-virus software helps to protect your computer from viruses. Viruses today can steal your personal data, utilize your computer’s resources to send spam, slow down and crash your computer, permit an unauthorized user access to your internet connection (for things such as illegal downloads), and many other malicious things. In order to protect against the latest viruses, you must keep your software updated. Use automatic updates to help keep your software current, as it’s only as good as its last update.
4. **Install and maintain antispyware software** – Spyware is software installed without your knowledge or consent that can collect your personal information and monitor your online activity. Signs that your machine could be infected by spyware include sudden multiple pop up ads, slowed performance, or being redirected to a site you did not choose to go to. Some anti-virus software also includes anti-spyware software. Keep this software updated regularly to keep the latest invasion tactics out of your machine. To avoid spyware you shouldn’t click on links in emails from unknown senders and download software only from sites you know and

- 6. Always be wary of attachments** - Always make sure you know the sender prior to opening an attachment received in an email or an IM. Even if the attachment is sent from a trusted source, always read through the message that accompanies it, and if anything is suspect, don't open it. Many viruses propagate by sending themselves as email attachments to the host computer's entire address book.
- 7. Use flash drives cautiously** - Disable auto-run in Windows so nothing will automatically launch when you insert a new drive. Always perform a scan on flash drives prior to opening files saved on them. Never open files that you are not expecting to be on the device.
- 8. Operating System and Program Patches** - Knowing when to patch products and how often patches need to be applied are some of the questions that most home users never think about. More and more programs are now offering auto update of their software allowing for applying patches every time the program needs to be updated. Although these updates don't always mean it is for the sake of security, a security patch may be issued along with the update. Microsoft Windows offers windows updates automatically. So updating windows is easier than ever when users choose this option. Knowing what else to patch other than operating system patches is important as well. Any program that acts as a server or accesses the Internet are avenues for attack. These programs need to be patched when one is available. Programs like email, browsers, flash programs, PDF programs, etc. need to be patched if one is available. If any of your programs do not have auto update capabilities, it is a good idea to check for patches to your software products at least once per month. If you use your computer on a daily basis, or the computer stays online constantly, such as with high speed connections, you may need to consider a more aggressive schedule for patches.

*The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. Organizations have permission--and in fact are encouraged--to redistribute this newsletter in whole for educational, non-commercial purposes.*